SPYWOLF

Security Audit Report

ARENA OF FIGHTERS

Completed on
January 6, 2022

OVERVIEW

This audit has been prepared for **Arena of Fighters** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> – SPYWOLF Team –

SPYWOLF.CO

TABLE OF CONTENTS

ARENA OF FIGHTERS

Scroll do.

PROJECT DESCRIPTION

According to their whitepaper:

Arena of fighters will be a multiplayer TPS game of CGU mode that consists of elements like MOBA, RPG, Roguelike and Social, A competitive Web3 Battle ground, Play for Fun and Earn for real, ARENA ensure that the earning is easier through different gaming channels.

Release Date: Presale starts in January, 2023

Category: Play to earn (P2E)

01

CONTRACT INFO

Token Name
ARENA OF FIGHTERS TOKEN

Symbol
ARENA

Contract Address
0x1De4Dae1ef6E14E702be6f9fda91f3133be08c70

Network
Binance Smart Chain

Language
Solidity

Deployment Date
Jan 6, 2023

Verified?
Yes

Total Supply
100,000,000,000

Status
Not launched

TAXES

Buy Tax
10%

Sell Tax
10%

*Taxes can be changed in future

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

02

CURRENT STATS

(As of January 06, 2023)

Liquidity

Not added yet

Burn

No burnt tokens

Status:
Not Launched!

MaxTxAmount
10,000,000,000

DEX
PancakeSwap

LP Address(es)

Liquidity not added yet

03

TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	99999999999.99998 ARENA
Median Transfer Amount	99999999999.99998 ARENA
Average Transfer Amount	99999999999.99998 ARENA
First transfer date	2023-01-06
Last transfer date	2023-01-06
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-01-06 10:10:55 UTC
Created	2023-01-06 10:10:55 UTC
Create TX	0xf280a666a30146e3a5ddf8435d58583 4959d263bf58808a29693c48934eec8c3
Creator	0x9ed8d866e723d69479a39b146dfed27 3964172f7

04

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

05

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

06

FOUND THREATS

⚠️ High Risk

No high risk-level threats found in this contract.

⚠️ Medium Risk

No medium risk-level threats found in this contract.

⚠️ Low Risk

No low risk-level threats found in this contract.

07-A

ℹ️ Informational

Owner can exclude address from fees.

```solidity
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}
```

Owner can set max transaction limit but can't lower it than 0.2% of total supply.

```solidity
function setMaxTxAmount(uint256 newNum) external onlyOwner() {
    require(newNum >= (totalSupply() * 2 / 1000),
    "Cannot set maxTransactionAmount lower than 0.2%");
    _maxTxAmount = newNum;
}
```

07-B

ℹ️ Informational

Owner can set buy/sell fees up to 12%.
Combined buy+sell=24%.

```solidity
function setTaxFeePercent(uint256 taxFee, uint256 marketingFee,
uint256 devFee, uint256 liquidityFee) external onlyOwner() {
    _taxFee = taxFee;
    _marketingFee = marketingFee;
    _devFee = devFee;
    _liquidityFee = liquidityFee;

    totalFees = _taxFee + _marketingFee + _devFee + _liquidityFee;

    require(totalFees <= 12, "Must keep fees at 12% or less");
}
```

07-C

RECOMMENDATIONS FOR
GOOD
PRACTICES

1. Consider fundamental tradeoffs

2. Be attentive to blockchain properties

3. Ensure careful rollouts

4. Keep contracts simple

5. Stay up to date and track development
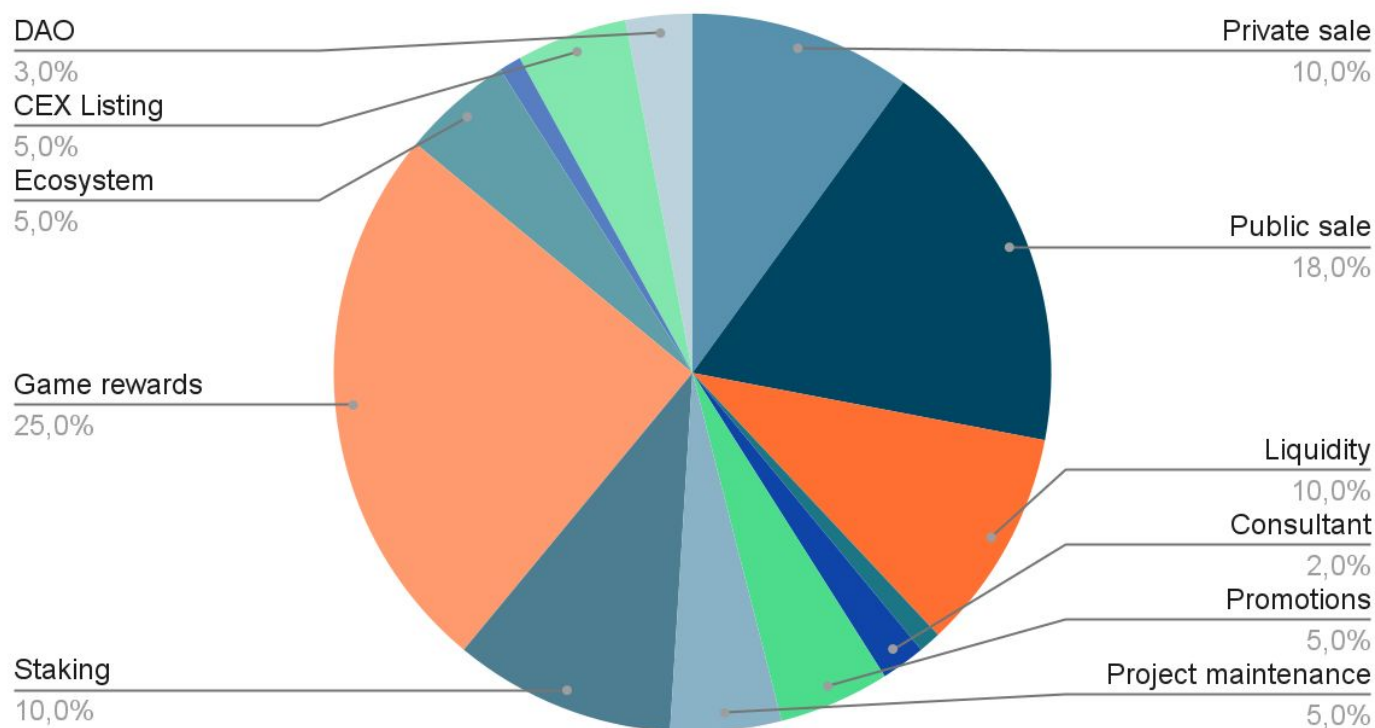
ARENA OF FIGHTERS

GOOD PRACTICES FOUND

✔ The owner cannot mint new tokens after deployment

✔ Owner can set max transaction limit, but cannot lower it than 0.2% of total supply.

✔ The smart contract utilizes "SafeMath" to prevent overflows

08

The following tokenomics are based on the project's whitepaper and/or website:

- 10% - Private sale
- 18% - Public sale
- 10% - Liquidity
- 10% - Staking
- 5% - CEX listing
- 5% - Promotions
- 1% - Airdrop

- 25% - Game rewards
- 5% - Ecosystem
- 2% - Consultant
- 3% - DAO
- 1% - Test & Bounty plan
- 5% - Project maintenance

Tokens distribution

DAO
3,0%

CEX Listing
5,0%

Ecosystem
5,0%

Game rewards
25,0%

Staking
10,0%

Private sale
10,0%

Public sale
18,0%

Liquidity
10,0%

Consultant
2,0%

Promotions
5,0%

Project maintenance
5,0%

THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

10

Website URL
https://arenaoffighters.com/

Domain Registry
https://www.gandi.net

Domain Expiration
Expires on 2023-12-17

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
Single page design with nice color scheme and overall layout.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.
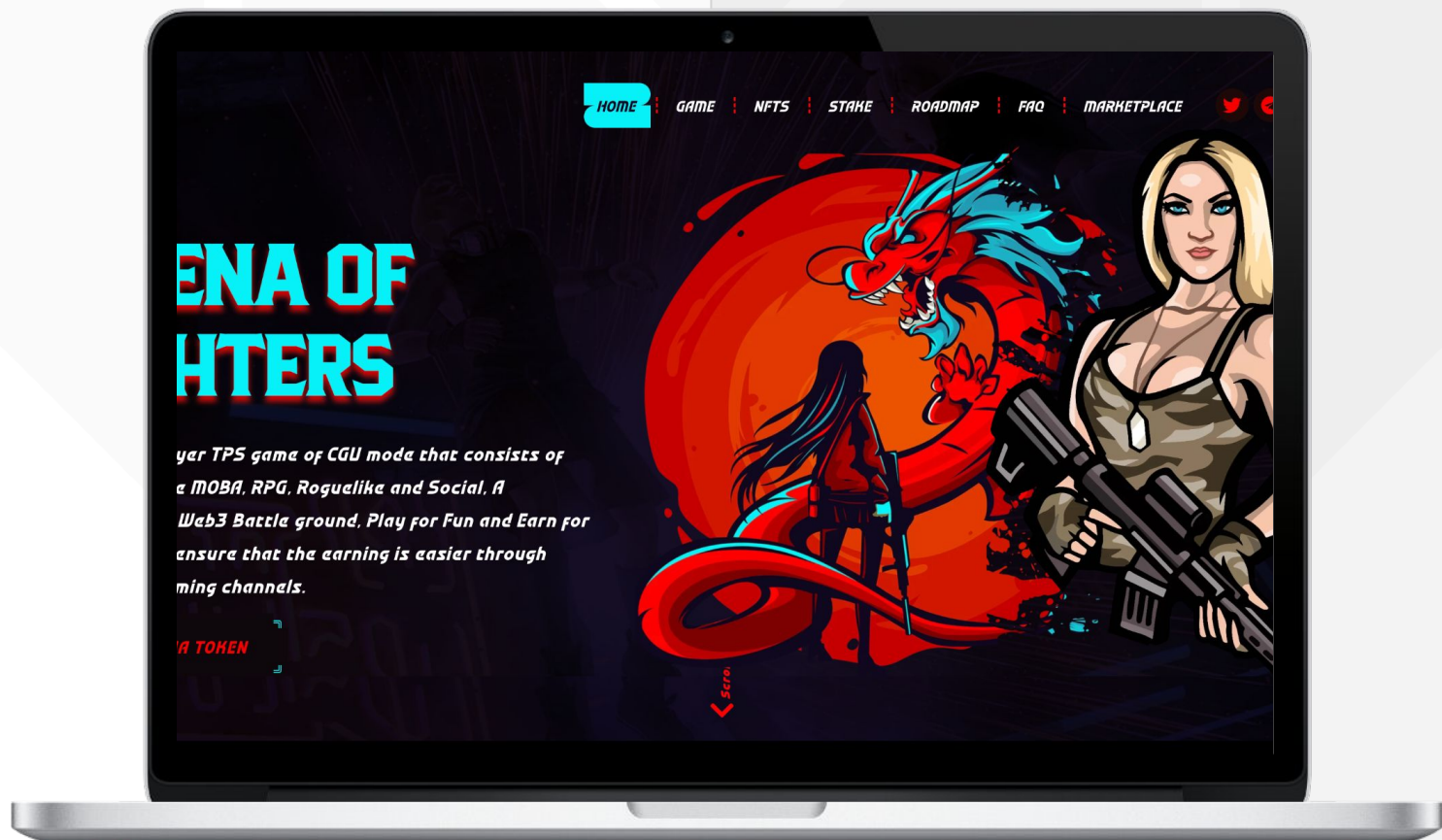
Whitepaper
Well written explanatory.

Roadmap
Yes, goals set in 3 phases.
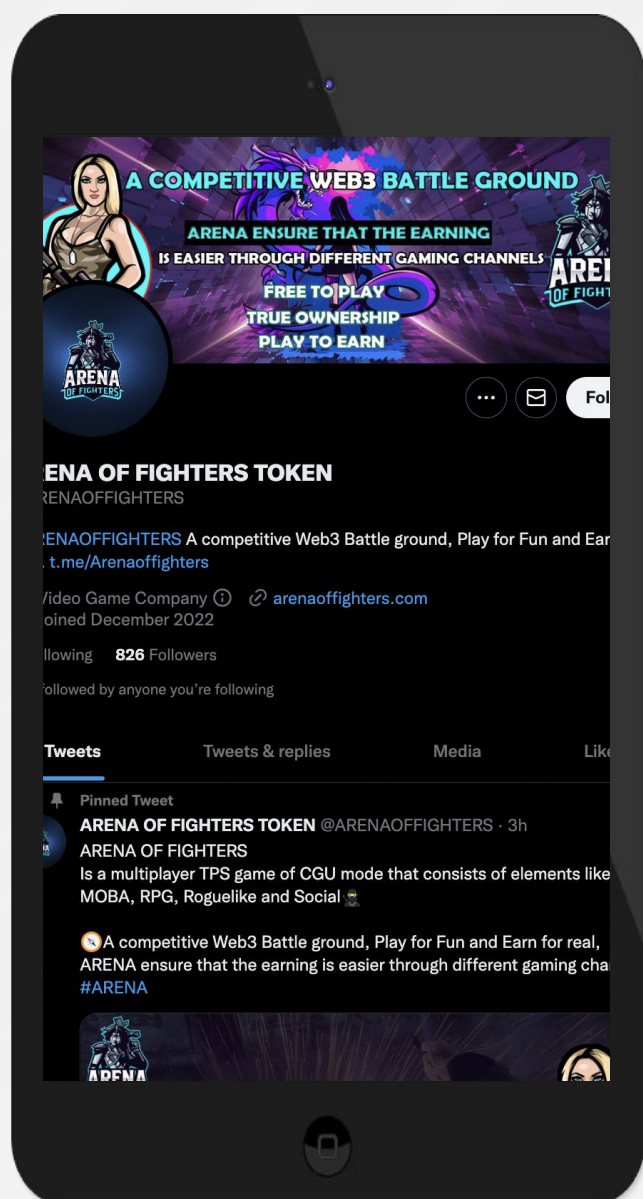
Mobile-friendly?
Yes

11

arenaoffighters.com
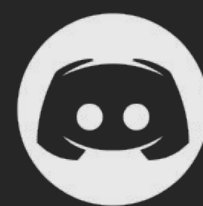
SOCIAL MEDIA

& ONLINE PRESENCE

Twitter

@ARENAOFFIGHTERS

- 3 173 followers
- Active
- Daily posts

Discord

- Not available

Telegram

@Arenaoffighters

- 15 361 members
- Few active organic members
- Active mods

Medium

- Not available

12

SPYWOLF
CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✔ **OVER 150 SUCCESSFUL CLIENTS**

- ✔ **MORE THAN 500 SCAMS EXPOSED**

- ✔ **MILLIONS SAVED IN POTENTIAL FRAUD**

- ✔ **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**

- ✔ **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to contact@spywolf.co or t.me/joe_SpyWolf

FIND US ONLINE

🌐 **SPYWOLF.CO**

🌐 **SPYWOLF.NETWORK**

✈ **@SPYWOLFNETWORK**

✈ **@SPYWOLFOFFICIAL**

🐦 **@SPYWOLFNETWORK**

⊙ **@SPYWOLFNETWORK**

13

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.